The Youth Cybersecurity Concepts Instrument (YCCI): Developing a Scale for the GenCyber Cybersecurity Concepts

Completed paper

Justin Scott Giboney
Brigham Young University
justin_giboney@byu.edu

Ersin Dincelli
University of Colorado Denver
ersin.dincelli@ucdenver.edu

Geoff Wright
Brigham Young University
geoffwright@byu.edu

Quincy Taylor
Brigham Young University

Dallin Christensen
Brigham Young University

ABSTRACT

There are many efforts to increase the cybersecurity workforce. GenCyber is the largest sponsor of cybersecurity youth camps, hosting over 160 summer camps a year. The goal of GenCyber is to: (1) Ignite, sustain, and increase awareness of K12 cybersecurity content and cybersecurity postsecondary and career opportunities for participants through year-round engagement; (2) Increase student diversity in cybersecurity college and career readiness pathways at the K-12 level; and (3) Facilitate teacher readiness within a teacher learning community to learn, develop, and deliver cybersecurity content for the K-12 classroom in collaboration with other nationwide initiatives (https://www.gen-cyber.com/about/). To accomplish their goal, they have six primary cybersecurity concepts students are exposed to and learn: confidentiality, integrity, availability, defense in depth, adversarial thinking, and keep it simple. With no current way to measure knowledge of these concepts in camp attendees, this research introduces the Youth Cybersecurity Concept Instrument (YCCI). The instrument was reviewed and validated by ten cybersecurity and pedagogy experts. During a 2021 and 2022 GenCyber camp, the research team administered a pre

and post YCCI to 162 camp attendees. After disaggregating the data, the research team noticed an increase in the post-camp measurement, suggesting that the YCCI effectively measures knowledge of fundamental cybersecurity concepts.

Keywords

GenCyber, CIA triad, Adversarial thinking, Defense-in-depth, Keep it simple, Girls in cybersecurity.

INTRODUCTION

According to the (ISC)² Cybersecurity Workforce Study, the cybersecurity field has a growing workforce gap that totaled approximately 3.1 million skilled cybersecurity professionals in 2020 (ICS2 2020). Several reasons constitute the workforce gap in the cybersecurity field, such as the lack of: interest, understanding, and diversity (Gonzalez 2015). Therefore, educating a new generation of cyber workers to address the growing cybersecurity workforce gap is an urgent, yet challenging, need to improve the cybersecurity posture of organizations and nations (Crumpler and Lewis 2019).

There are various programs dedicated to increasing interest in cybersecurity and drawing diverse talent to the cybersecurity career paths. These programs are tailored toward young generations. One such program is the GenCyber program. The GenCyber program is jointly sponsored by the National Science Foundation (NSF) and National Security Agency (NSA). The GenCyber program has two primary (and complementary) aims: (1) to provide K-12 students and teachers with summer cybersecurity camp experiences and (2) address the nationwide shortage of skilled cybersecurity professionals.

The GenCyber program has established a set of six cybersecurity concepts for attendees to learn: Confidentiality, Integrity, Availability, Defense in Depth, Adversarial Thinking, and Keep it Simple. However, to our knowledge, there is no scale instrument designed to measure these six concepts for youth. This research aimed to develop and validate a measure to accurately assess a youth cybersecurity novice's ability to recognize the six cybersecurity concepts. The remainder of this paper will review GenCyber and various cybersecurity fundamental topics. Then, the paper will introduce the instrument and describe the validation and deployment of the instrument. Finally, the paper will discuss the implications of the findings for both researchers and practitioners.

LITERATURE REVIEW

GenCyber

Cybersecurity skills are best acquired with experiential learning in an engaging classroom setting that uses real-life examples (Dark 2014). Accordingly, most of the GenCyber camps adopt hands-on exercises that are tailored towards young generations, such as game-based learning, challenge-based learning, and hands-on computer labs (Smith and Ali 2019). For example, Ford et al. (2017) developed an age-appropriate Capture the Flag (CTF) project. They found that GenCyber students who participated in the CTF demonstrated significant knowledge gain as well as confidence and comfort in participating in the competition. Jin et al. (2018) developed a GenCyber camp following a game-based learning methodology using various games. They found out that the students perceived game-based training as enjoyable and interesting. Ford and Siraj (2019) developed a gamified web platform called GenCyberCoin that complimented their camp materials. GenCyberCoin allowed students to engage in various hands-on activities.

The GenCyber program emphasizes the measurement of learning outcomes and evaluation. Although the program offers a site visit observation team that consists of pedagogy experts and conducts a survey to measure students' interest in cybersecurity, institutions are also required to evaluate their own camps. For example, Payne et al. (2016) administered a three hour Certified Ethical Hacker (CEH) exam on the last day of their camp. 22.5% of the students successfully passed the CEH exam. Similarly, Yan et al. (2021) developed the Cybersecurity Judgement Questionnaire (CJQ) to measure camp participants' rational and intuitive judgments of cybersecurity risks. They administered CJQ in 45 GenCyber camps (n=2,703) and identified critical cybersecurity risks and protective factors. Most of the literature found concerning measures associated to GenCyber focused on pedagogical and instruction practices used in the camps. For example, Jin et al. (2018) surveyed their camp attendees about the use of game-based learning. In summary, after researching various avenues of GenCyber we were unable to identify measures of the core cybersecurity concepts GenCyber asked to be included in the camps.

Cybersecurity Fundamentals

GenCyber is not the only source of these cybersecurity fundamentals. Many practitioner certifications contain similar if not the same concepts. Certifications designed for beginners approach a broad spectrum of topics. The GIAC's Information Security Fundamentals, CompTIA's Security+, $(ISC)^2$'s Systems Security Certified Practitioner, and the EC-Council's Certified Secure Computer User expect that beginners understand the six concepts GenCyber also uses. These certifications set these concepts in information technology topics such as networking and operating systems. These certifications also introduce the management of access controls on an enterprise scale and discuss confidentiality, integrity, and availability in terms of access. For defense in depth, these exams cover incident response operations and basic

overviews of common attack types and vulnerabilities. For confidentiality, cryptography is consistently covered by exams specifically focusing on the modern applications. Certificates also require students to demonstrate an understanding of the principle of risk, enterprise governance, and compliance.

SCALE DEVELOPMENT

Measure background

GenCyber has two different topic sets that camp organizers can have in their camps: GenCyber Cybersecurity First Principles and GenCyber Cybersecurity Concepts. This research focuses on the latter. GenCyber (2020) has provided definitions for the Cybersecurity Concepts (p. 28-29): *Confidentiality* – The property that information is not disclosed to individuals, devices, or processes unless they have been authorized to access the information. *Integrity* – The property that information, an information system, or a component of a system has not been modified or destroyed in an unauthorized manner. *Availability* – The property that information or information systems are accessible and usable upon demand. *Defense in Depth* – A comprehensive strategy of including multiple layers of security within a system so that if one layer fails, another layer of security is already in place to stop the attack/unauthorized access. *Think Like an Adversary (Adversarial Thinking)* – The strategy of putting yourself inside the mindset of a potential attacker that allows you to anticipate attack strategies and defend your systems accordingly. *Keep It Simple* – The strategy of designing information and security systems to be configured and operated as simply as possible; all systems perform best when they have simple designs rather than complex ones.

Scenario generation

To measure the GenCyber Cybersecurity Concepts understanding of camp attendees, we developed an instrument called the Youth Cybersecurity Concepts Instrument (YCCI). Because the instrument was targeted for youth, we included vivid colors and visuals in the design of the instrument so that the participants are less likely just to skim the text (Dincelli and Chengalur-Smith 2020). We deemed that a story-to-concept matching-style scale would be easy to use for the participants. We created eight scenarios using situations from the lives of youth that they would likely relate to. Each scenario relates to one to two of the GenCyber Cybersecurity Concepts. Specifically, Sarah's scenario focuses on: Confidentiality, Josephine's scenario concerns Integrity, Bobby's scenario is about Adversarial Thinking, Smith's scenario focuses on Defense in Depth, Josh's concerns Availability, Janet's scenario concerns Keep it Simple and Confidentiality, and Wendy's scenario focuses on Defense in Depth. We also designed an additional scenario that did not involve a cybersecurity concept to introduce a control variable, that scenario was Josh's. See **Figure 1** for the instrument.

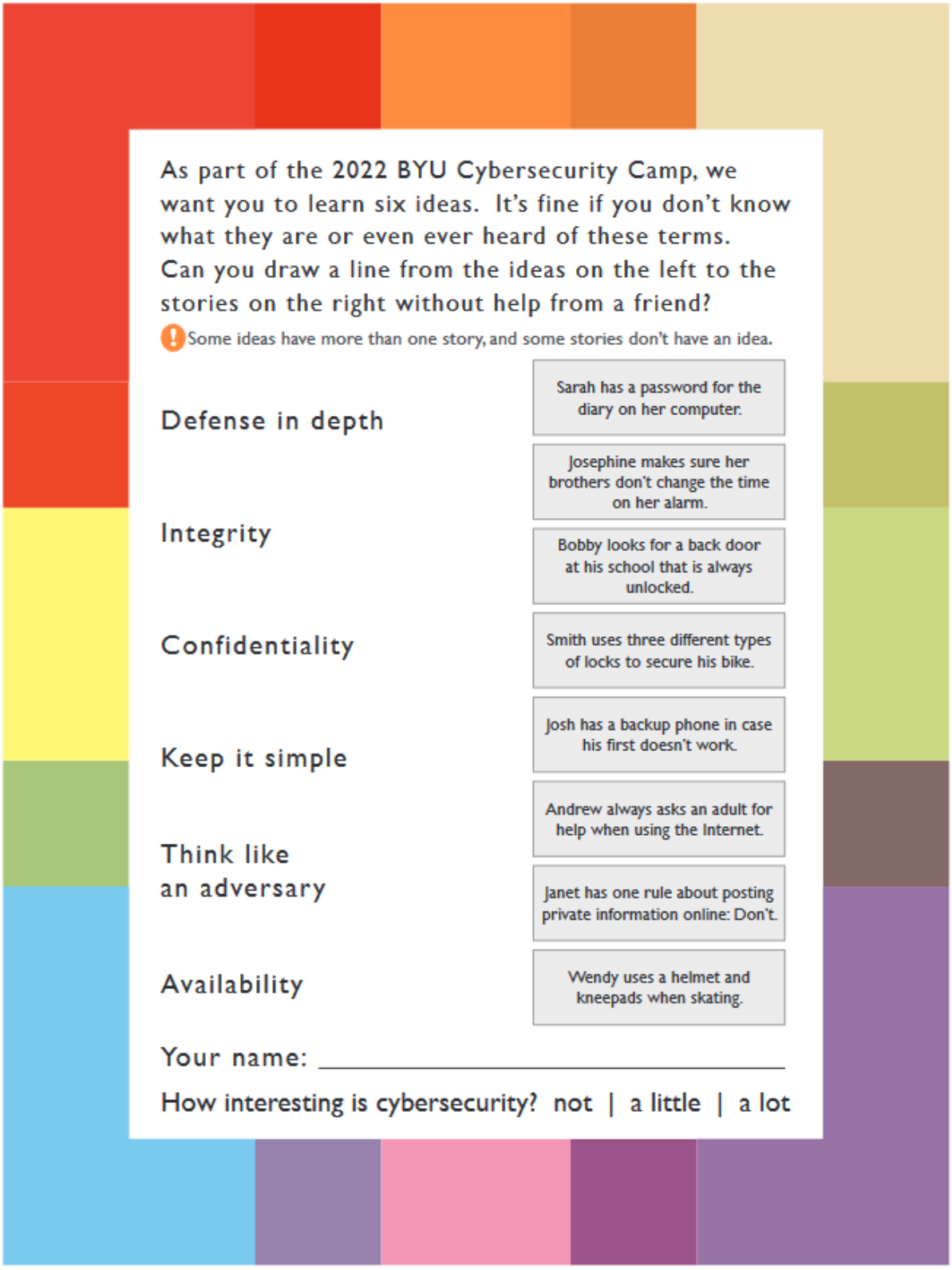

Figure 1. GenCyber Youth Cybersecurity Concepts Instrument (YCCI)

Assessing content validity

To scientifically validate the YCCI, we had ten experts review and empirically validate the scale using an item-ranking task recommended by MacKenzie et al. (2011). First, our experts reviewed the content validity of the scenarios and indicated that the items seemed appropriate. Second, we validated the items by asking the experts to rate how well each of the scenarios matches with each of the concepts. To show empirical validation, each scenario should be rated highly on the concept(s) of interest and be rated low on all the other concepts. MacKenzie et al. (2011) recommended a technique by Hinkin and Tracey (1999) where the experts use a matrix with scenarios as rows and concepts as columns and the experts provide a five-point number (1 = does not fit; 5 = completely fits) for each pairing. We provided a hypothetical example of the item-ranking task in Table 1.

Table 1. **A hypothetical example of the item-ranking task.**

Rater # = 001	Confiden-tiality	Integrity	Availabil-ity	Defense in Depth	Adversar-ial Thinking	Keep it Simple
Sarah has a password for the diary on her computer.	4	2	1	1	1	2
…	…	…	…	…	…	…
Wendy uses a helmet and kneepads when skating.	2	1	1	5	1	2

Using the data provided by the experts, we performed a one-way repeated measures ANOVA for each scenario as recommended by MacKenzie et al. (2011). A significant result from the ANOVA indicates that at least one of the concepts was rated differently from the others for that scenario.

To identify whether the concept of interest is different than the others, MacKenzie et al. (2011) recommend using a second one-way repeated ANOVA using planned contrasts. We performed both ANOVAs and reported the results in Table 2.

Table 2. **Means and ANOVA results of content validity reviewers.**

Scenario	Confide-ntiality	Integrity	Availa-bility	Defense in depth	Advers-arial thinking	Keep it simple	ANOVA p-value	Planned contrast p-value
Sarah	**4.8**	2.7	2.2	2.7	1.6	2.4	5.0e-5	1.3e-6
Josephine	1.1	**4.5**	2.8	1.2	3.8	1.9	3.3e-10	1.0e-5
Bobby	1.4	1.3	2.7	1.9	**4.7**	1.9	1.4e-8	1.4e-9
Smith	1.4	1.4	2.1	**4.7**	2.4	1.6	5.6e-9	1.2e-10
Josh	1.0	1.7	**4.1**	2.4	1.5	1.7	3.2e-6	1.2e-10
Andrew	1.1	1.0	1.0	1.8	1.6	1.8	2.6e-2	7.0e-2
Janet	**4.6**	1.6	1.8	2.0	3.3	**4.4**	2.6e-7	6.7e-4
Wendy	1	1.8	1.7	**3.3**	1.6	2.4	5.4e-4	1.4e-4

Bolded cells are those of interest for each scenario.

SCALE EVALUATION

To evaluate YCCI, we administered a pre- and post-test to attendees (age 10-18) of three week-long GenCyber camps. The first one occurred in 2021 with 98 girls. The second, occurred in 2022 with 82 boys. The third, was also in 2022 with 66 girls. As the youth came on the first day of camp, they were physically handed the instrument. The instrument was collected 30 minutes after the start of camp. Just before the award ceremony on the last day of camp, the youth were again physically handed the instrument to do a second time. There was no specific discussion of the instrument during camp at any time. We covered many of the principles measured in the instrument, but no reference was made to the instrument itself. There were 94 girls that completed at least the pre or post survey in 2021, 65 girls in 2022, and 83 boys in 2022. 64 girls completed both the pre and the post measurement in 2021, 37 girls in 2022, and 61 boys. This was largely due to youth not attending the first or last day of the camp.

To test the effectiveness of the instrument, we ran a *t*-test between the pre-camp measurement and the post-camp measurement. The *t*-test showed an increase between the two measurements ($t = -2.10$, $p = 0.037$; see Figure 2). Specifically, the mean before the camp score was 3.49 and the mean after the camp score was 3.86. The increase in score indicates that we measured a phenomena that most likely increased during camp. We contend that the phenomena is: an increase in the understanding of the six GenCyber Cybersecurity Concepts. The significance shows the accuracy of the scale in measuring understanding of the GenCyber Cybersecurity Concepts.

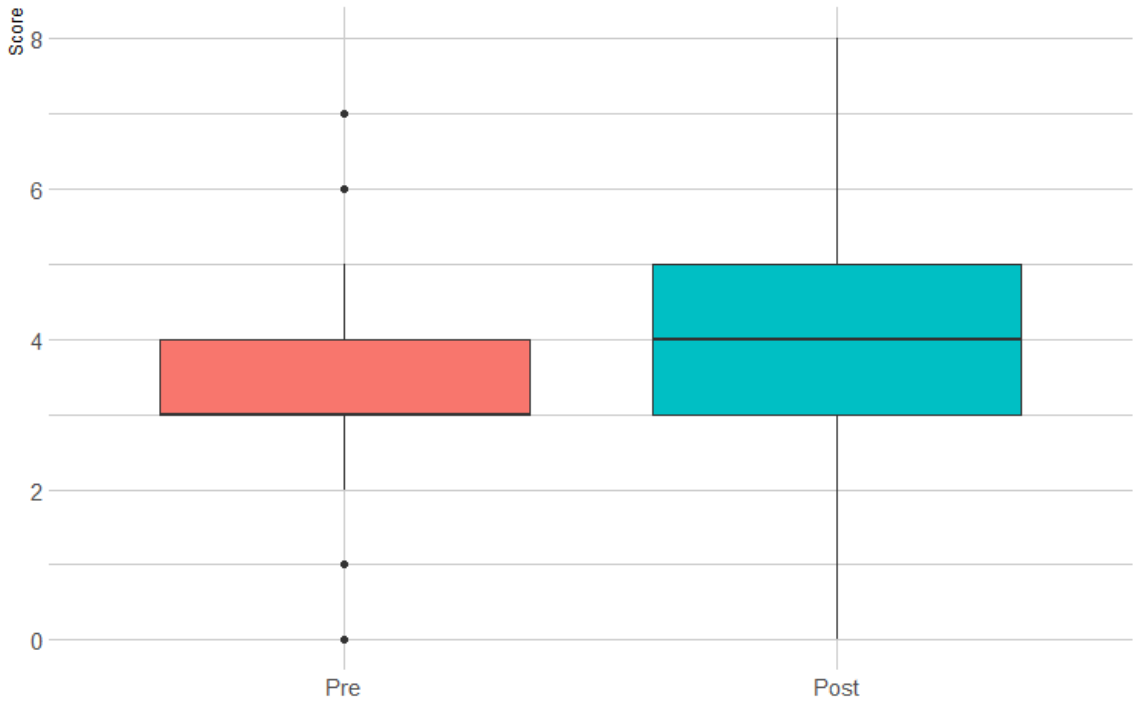

Figure 2. **Scale results before and after camp.**

DISCUSSION

Limitations

Before discussing the implications of this research, we want to acknowledge some limitations. First, this research was conducted at a single U.S. university with a sample of youth interested enough to come to a cybersecurity camp. While most of the girls reported little-to-no knowledge of cybersecurity before camp, it is still likely a biased sample. Second, the instrument was physically handed to the participants. Papers were drawn on and hand coded. Errors are possible. Lastly, participants were not told the instrument was a test, rather a simple activity that was part of the camp – therefore we cannot be sure of how serious or how much effort the students put in to completing the instrument.

Implications for research

The main research contribution of this paper is the development and validation of an instrument to measure cybersecurity concepts encapsulated in the YCCI. Measurement of cybersecurity knowledge can be difficult (Giboney et al. 2016), especially in youth. This paper presents the YCCI as an easy-to-implement measure for youth. Future research will benefit from the YCCI to measure cybersecurity training in novices. This research provides a foundational tool for researchers that hope to measure antecedents or aftereffects of GenCyber cybersecurity concept knowledge.

Implications for practice

The main benefit of this research for practice is the ability of cybersecurity camps to use YCCI to measure the knowledge of GenCyber Cybersecurity Concepts among attendees. GenCyber funded over 160 camps in 2021. GenCyber funding and the number of camps will continue to grow for the foreseeable future. These camps can use the YCCI to measure the effectiveness of their educational experience.

CONCLUSION

There are many efforts to increase the cybersecurity workforce; from educational games (Giboney et al. 2021) to cybersecurity camps for youth (c.f., Ivy et al. 2020). GenCyber is the largest sponsor of cybersecurity youth camps. GenCyber wants their camps to teach six cybersecurity concepts. However, there is no measure for how well participants learn these concepts during camp. This research introduces the Youth Cybersecurity Concept Instrument (YCCI) to measure knowledge of these concepts. During a GenCyber camp, the research team administered a pre-camp measurement and a post-camp measurement. Expert validation and an increase in the post-camp

measurement suggests that the YCCI is effective at measuring knowledge of fundamental cybersecurity concepts.

REFERENCES

Crumpler, W., and Lewis, J. A. 2019. "The Cybersecurity Workforce Gap."

Dark, M. 2014. "Advancing Cybersecurity Education," *IEEE Security & Privacy* (12:6), IEEE, pp. 79–83. (https://doi.org/10.1145/2538029).

Dincelli, E., and Chengalur-Smith, I. 2020. "Choose Your Own Training Adventure: Designing a Gamified SETA Artefact for Improving Information Security and Privacy through Interactive Storytelling," *European Journal of Information Systems* (29:6), Taylor & Francis, pp. 669–687. (https://doi.org/10.1080/0960085X.2020.1797546).

Ford, V., and Siraj, A. 2019. "GenCyberCoin: An Engaging, Customizable, and Gamified Web Platform for Cybersecurity Summer Camps and Classrooms," *Journal of Computing Sciences in Colleges* (35:3), pp. 87–96.

Ford, V., Siraj, A., Haynes, A., and Brown, E. 2017. "Capture the Flag Unplugged," in *ACM SIGCSE Technical Symposium on Computer Science Education*, pp. 225–230. (https://doi.org/10.1145/3017680.3017783).

GenCyber. 2020. "2020 GenCyber Call for Proposals."

Giboney, J. S., McDonald, J. K., Balzotti, J., Hansen, D. L., Winters, D. M., and Bonsignore, E. 2021. "Increasing Cybersecurity Career Interest through Playable Case Studies," *TechTrends*. (https://doi.org/10.1007/s11528-021-00585-w).

Giboney, J. S., Proudfoot, J. G., Goel, S., and Valacich, J. S. 2016. "The Security Expertise Assessment Measure (SEAM): Developing a Scale for Hacker Expertise," *Computers & Security* (60), Elsevier Ltd, pp. 37–51. (https://doi.org/10.1016/j.cose.2016.04.001).

Gonzalez, M. D. 2015. "Building a Cybersecurity Pipeline to Attract, Train, and Retain Women.," *Business Journal for Entrepreneurs* (2015:3), pp. 24–41.

Hinkin, T. R., and Tracey, J. B. 1999. "An Analysis of Variance Approach to Content Validation," *Organizational Research Methods* (2:2), pp. 175–186.

ICS2. 2020. "Cybersecurity Professionals Stand Up to a Pandemic - Cybersecurity Workforce Study, 2020," *The International Information System Security Certification Consortium Research*.

Ivy, J., Kelley, R., Cook, K., and Thomas, K. 2020. "Incorporating Cyber Principles into Middle and High School Curriculum," *International Journal of Computer Science Education in Schools* (4:2), pp. 3–23. (https://doi.org/10.21585/ijcses.v4i2.101).

Jin, G., Tu, M., Kim, T.-H., Heffron, J., and White, J. 2018. "Evaluation of Game-Based Learning in Cybersecurity Education for High School Students," *Journal of Education and Learning (EduLearn)* (12:1), pp. 150–158. (https://doi.org/10.11591/edulearn.v12i1.7736).

Mackenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. "Construct Measurement and

Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques," *MIS Quarterly* (35:2), pp. 293–334.

Payne, B., Abegaz, T., and Antonia, K. 2016. "Planning and Implementing a Successful NSA-NSF GenCyber Summer Cyber Academy," *Journal of Cybersecurity Education, Research and Practice* (2016:2), p. 3.

Smith, D. T., and Ali, A. I. 2019. "You've Been Hacked: A Technique for Raising Cyber Security Awareness," *Issues in Information Systems* (20:1), pp. 186–194.

Yan, Z., Xue, Y., and Lou, Y. 2021. "Risk and Protective Factors for Intuitive and Rational Judgment of Cybersecurity Risks in a Large Sample of K-12 Students and Teachers," *Computers in Human Behavior* (121), Elsevier Ltd, p. 106791. (https://doi.org/10.1016/j.chb.2021.106791).